UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,238	04/01/2000	Srinivas Chaganty	M-8403 US	9955

7590 11/12/2003

Avaya Inc.
Docket Administrator
P.O. Box 629
Holmdel, NJ 07733

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2131	19

DATE MAILED: 11/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/540,238	CHAGANTY ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-63 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-63 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-63 have been re-examined.

2. The objected Specification and claims 48-62 are withdrawn.

3. Claim 43 was rejected under 35 U.S.C. 112, 1st paragraph is now withdrawn.

4. Claims 1-7, 14-19, 23-30, and 37-63 remains rejected under 35 U.S.C. 102(e).

5. Claims 8-13, 20-22, and 31-36 remains rejected under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1-7, 14-19, 23-30, and 37-63 are rejected under 35 U.S.C. 102(e) as being unpatentable over Coile, et al. (US 6,108,300).

As per claims 1 and 16:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44).

Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). Therefor, it is inherent that plurality of firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there exists a primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC

address of a functional backup network device is adopted and the MAC address of the failed network device is no longer in use (col.5, lines 55-58). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address. The Examiner further asserts that each of the firewalls have a different fixed MAC address so when one firewall fails, it is directed to the active firewall therefore adopting the MAC address of the active firewall.

As per claim 2: See col.5, lines 26-31 discussing the plurality of servers.

As per claim 3:

Coile discuss each switch is associated with each connection where different network devices is connected at different ports (col.10, lines 32-43). Therefore, it is inherent to relay the packets to the functional firewalls over unshared ports so that packets can be forwarded to the standby device without confusion of which network device location has failed (col.10, lines 26-30).

As per claim 4: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claims 5: See col.11, lines 2-8 discussing the ARP request.

As per claim 6:

Coile suggests ARP but fails to describe the functions of an ARP in more detail. The Examiner asserts the use of ARP request is to determine the physical address of a node. The Examiner asserts it is inherent the function of

an ARP request of Coile's invention is to find out the new address of the functional firewall (col.12, lines 42-44). Therefore, Coile inherently teaches responding to the ARP requests with an active MAC address of a firewall.

As per claim 7:

Coile teaches the use of the PING test during a 5 seconds interval to determine if the remote device has failed (col.11, lines 10-25). The Examiner asserts that Coile suggests the ICMP. As understood by the Examiner, Ping is to see whether the machine is connected to a destination such as the Internet and ICMP communicates errors and informs machines about an unreachable destination. Therefore, the ICMP method for determining whether the particular destination is reachable or operational.

As per claim 14: See col.6, lines 14-19 discussing transferring the packets between the server and a firewall.

As per claim 15: See col.13, line 8.

As per claim 16:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44).

Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). Therefor, it is inherent that plurality of

firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there exists a primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device is adopted and the MAC address of the failed network device is no longer in use (col.5, lines 55-58). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address. The Examiner further asserts that each of the firewalls have a different fixed MAC address so when one firewall fails, it is directed to the active firewall therefore adopting the MAC address of the active firewall.

As per claim 17: See col.11, lines 2-8 discussing the ARP request.

As per claim 18: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claim 19: See col.13, line 8.

As per claim 23:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network that is coupled to the backbone of the Internet (col.12, line 65 – col.13, line 4). The network includes servers **210,220** and a switch circuit in the form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). Further, it is inherent that plurality of firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there is MAC address for each primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore,

the packets are relayed to the functional network device with the active MAC address.

As per claim 24: See col.5, lines 26-31 discussing the plurality of servers.

As per claim 25: See col.12, lines 10-41 discussing the failover cable relaying the packet to the second firewall with a fixed MAC address.

As per claim 26:

Coile discusses the network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67).

As per claim 27: See col.11, lines 2-8 discussing the ARP request.

As per claim 28: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claim 29: See col.11, lines 3-8 discussing monitoring responses.

As per claim 30:

Coile discusses that once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address.

As per claim 37: See col.6, lines 14-19 discussing transferring the packets between the server and a firewall.

As per claim 38: See col.7, lines 35-52 discussing full duplex between the firewall and the server.

As per claim 39: See col.13, line 8.

As per claim 40:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). The failover cable is plugged on each side of the firewalls (col.7, lines 35-52) and the network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Coile fails to suggest sending a request message to a second side of the firewall. It is inherent if Coile can send a request message through the firewall by having the MAC address, then it is possible to send a

request message by using the MAC address to get to the location or to any side of the firewall. See Fig.1

As per claim 41: See col.13, lines 12-21 and FIG.9 discussing the first memory and the second memory.

As per claim 42: See col.13, lines 12-21 discussing each session between computers.

As per claim 43:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). The failover cable is plugged on each side of the firewalls (col.7, lines 35-52) and the network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Coile fails to suggest sending a request message to a second side of the firewall. It is inherent if Coile can send a request message through the firewall by having the MAC address, then it is possible to send a

request message by using the MAC address to get to the location or to any side of the firewall. See Fig.1

As per claim 44: See col.6, lines 43-59 discussing the failover cable generates, sends, and processes.

As per claim 45:

Coile teaches the use of NAT where the invention of Coile translates the packet addresses (col.5, lines 60-61).

As per claim 46: See col.10, lines 39-42 discussing receiving and replying a request on a port.

As per claim 47:

Differs from claim 23, wherein the network includes a second switch circuit (col.10, lines 30-34).

As per claim 48: See col.12, lines 25-27 discussing the plurality of first computers couple to the failover cable and its MAC address.

As per claim 49: See col.5, lines 55-58 discussing the second computers.

As per claim 50: See col.5, lines 44-45.

As per claim 51:

Coile discloses a flash memory device for storing programs or data (col.13, lines 13-14). It is inherent that a memory can have multiple storage elements to store the different data needs.

As per claim 52: See col.6, lines 43-59 discussing detecting and sending request message to the firewalls wherein the absence of the confirmation message indicates it has failed.

As per claim 53:

Coile discloses request message by ping and ARP methods, however, Coile fails to particularly suggest ICMP, for ICMP is similar to the ping method but differs that it performs error correction. The Examiner asserts that both methods are used to determine whether a destination can be reached and provides the status of the firewalls.

As per claim 54:

Coile discloses changing address portion of a packet when the backup server is active (col.12, lines 24-32). Otherwise, the Examiner asserts the packet will resume the original address and that it is not necessary to modify the packet if the first firewall is functional.

As per claim 55: See col.12, lines 15-22 discussing replacing each received packet with the fixed MAC address of a functional firewall.

As per claim 56: See col.6, lines 2-3.

As per claim 57:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network. Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which

includes firewalls (col.5, lines 7-12). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). See Fig.1

As per claim 58: See col.7, lines 36-52 discussing the switch circuit performs detection.

As per claim 59: See FIGURES 8 and 9.

As per claim 60: See FIGURE 4 transferring the packets through a switch circuit.

As per claim 61:

Coile discloses a method of taking over the active IP address of the formerly active device that was deemed a failure. Therefore it is inherent that Coile does not change the IP address during the transferring of the packets to any of the firewalls. See col.12, lines 29-31.

As per claim 62:

The Examiner asserts it is inherent that Coile does not change the IP address during the transferring of the packets to any of the firewalls. See col.12, lines 29-31.

As per claim 63: See col.5, lines 55-65.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 8-13, 20-22, and 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coile, et al. and further in view of Belville, et al. (US 5,828,833).

As per claim 8:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 9:

As rejected in claim 8, and further includes where Belville discusses the cleanup thread including waiting for a time out period to pass (col.6, lines 56—63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because when the time out passes the privileges are allocated so the packet is not transferred to the non-operational firewall.

As per claim 10:

The same rationale applies to claim 9, and further includes the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all the known clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is more secure by having the advantage to have enough time and not less than the time period to learn the routes to all known clients. Else, there is no point for the recovered firewall to operate as securely as before. See col.5, lines 3-9 and col.12, lines 47-53.

As per claim 11:

The same rationale applies of claim 8, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 12:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the

system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). Also, see col.9, lines 3-17.

As per claim 13:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 20:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 21:

The same rationale applies of claim 20, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in

the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 22:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 31:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 32:

As rejected in claim 8, and further includes where Belville discusses the cleanup thread including waiting for a time out period to pass (col.6, lines 56—63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the

system of Coile, because when the time out passes the privileges are allocated so the packet is not transferred to the non-operational firewall.

As per claim 33:

The same rationale applies to claim 32, and further includes the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all the known clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is more secure by having the advantage to have enough time and not less than the time period to learn the routes to all known clients. Else, there is no point for the recovered firewall to operate as securely as before. See col.5, lines 3-9 and col.12, lines 47-53.as rejected on the same basis as claim 10.

As per claim 34:

The same rationale applies of claim 31, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 35:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 36:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no

response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

Minor Informalities

8. ***Claim 51 is objected to because of the following informalities:***

On line 6, the word "identify" should be "identity".

Appropriate correction is required.

Response to Argument

A thorough review of the prior art (Coile, Et Al.) proves that each of the firewalls have a "fixed" MAC address. The Examiner asserts that each firewall would have a fixed address and not a type of firewall where the MAC address would constantly change; the only change would be the packets. It would not be logical if the failed firewall takes on an address of an active firewall leaving that firewall that is really active with no responsibilities. Then the packets would still becoming to a failed firewall thinking it is going to an active firewall because of the active MAC address. The Examiner ascertains that once a firewall has failed the MAC address is no longer valid and the system would switch over to a firewall that is active in order to process the all the packets.

Coile teaches that upon detection of the failed firewall, the packet will "adopt" the MAC address of the active firewall. According to claim 1 on lines 8-15, states that to detect the packet directed to the failed firewall and changing the MAC address to an active firewall's address (col.5, lines 55-57). Coile does teach this on col.5, lines 57-60; where it intercept the packets and translates the packet addresses meaning changing the MAC address to the active MAC address of a functional firewall.

Please refer to Coile, Et Al. on col.5, Et SEQ. for more details concerning the rejections above.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

Lha

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100